

A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a blue gradient background, resembling a circuit board or a neural network.

THE ADVENTURES OF ANALYZING OLD MALWARE WITH NEW COMPUTERS

AN INCIDENT RESPONSE TALK?

- You might have been surprised at me giving an incident response talk, after previously giving Red Team oriented talks
 - Hacking Cloudpets
 - Phishing Github users with old blog posts
- I like to examine malware to see what attack methods they try to use
 - The attack methods can then be applied to red team activities

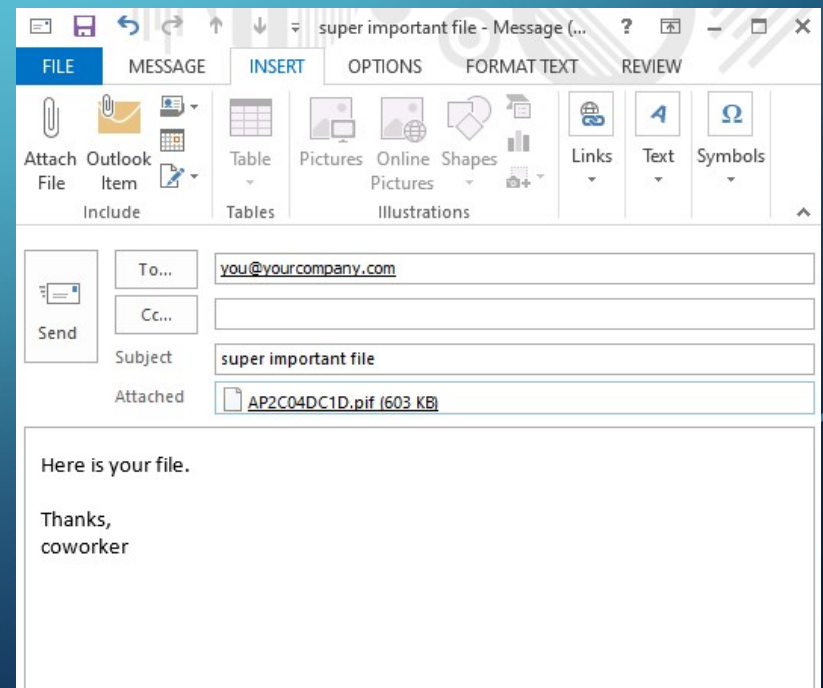
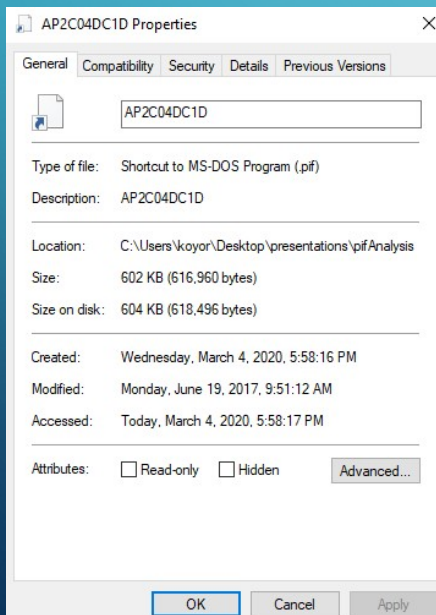
****Never hesitate to research and explore new topics**

DISCLAIMER

- Note: I am sure a malware analyst would be able to decipher most files' contents and actions at the assembly level
- But very few organizations have access to malware analysts / reverse engineers
- The rest of us try to fill in the gap with automated tools like malware sandboxes, virus total, etc

ANALYZING OLD MALWARE

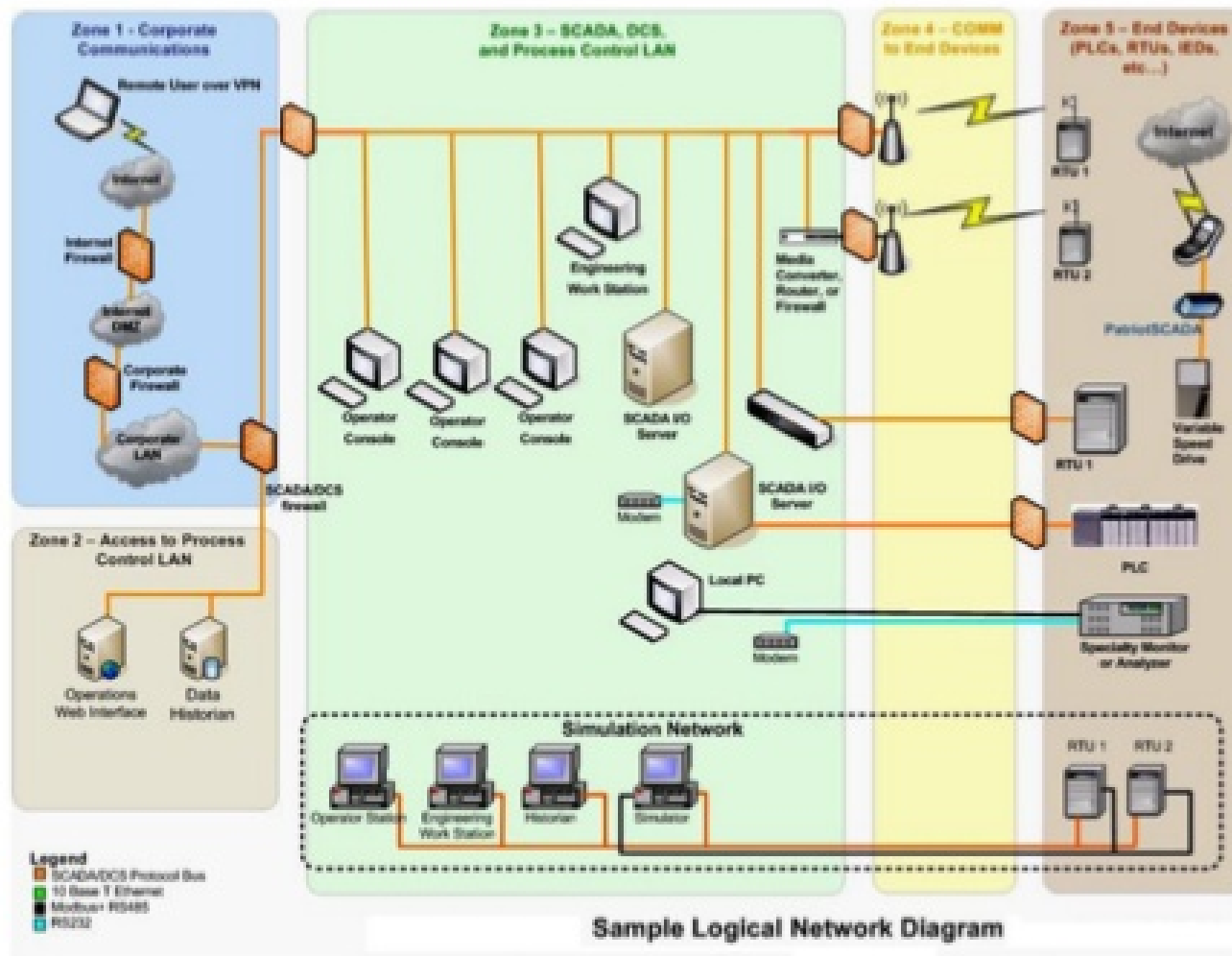
- An email attachment with a weird extension comes into your inbox
- You google the extension and find out it is an MSDOS shortcut file



ANALYZING OLD MALWARE

- Why would someone try to infect you with a 30 year old file format?
- A lot of critical systems still run on ancient operating systems
 - it is too risky to take the systems down to replace
 - or too costly to replace if the old system still works
 - or the manufacturer might not exist anymore to provide newer versions
- If an attacker can get a file onto the system, they can get foothold
 - Rob M Lee's RSA presentation on ICS vulns

SCADA Network... Isolation and Zoning



ANALYZING OLD MALWARE

- The .pif is normally just a text file that tells MSDOS how to open a file

.PIF File Extension

File Type

Program Information File



Developer N/A

Popularity  3.6 (23 Votes)

Category [Executable Files](#)

Format N/A

What is a PIF file?

A PIF file contains information used to define how an MS-DOS-based program should run. It can also serve as a shortcut to an executable file, much like a [.LNK](#) file, and is commonly created when the user makes a shortcut to a DOS program or modifies the properties of the program. PIF files contain various information such as the path for the [.EXE](#) file, how much memory to use, font size, screen colors, and the size of the program's window.

More Information

Microsoft Windows analyzes PIF files with the ShellExecute function and can run them as executable programs. Therefore, **do not open a PIF file sent as an e-mail attachment**, as it can be used to transmit [viruses](#) or other harmful scripts.

ANALYZING OLD MALWARE

- What tools are still available to analyze old files?
 - Nothing after Windows XP recognizes .pif files

ANALYZING OLD MALWARE

- What tools are still available to analyze old files?
 - Nothing after Windows XP recognizes
 - Try to go back to source OS: MSDOS
 - DOSBox emulator (since I didn't have access to MSDOS install media)



DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX



MZÉ ♥ ♦ 7 @
=!7@L=!This program cannot be run in DOS mode.
\$ 2-ö►||-C||-C||-Cu-²C||-C||JCO||-Cu-ñC||-Cu-ÑC||-Cu-áC||-CRich||-C
PE L@♥ 1{►A α *@δ@
Ü \d ► || @ ► @ ♣ @ ♣ @ ♦ ' ♦ 9^ @ ä ♦ ► ►
► ► Σf î || || 0† L
► 0@ .text ,ö ► Ü ♦
` .data Σ || ♦ R @ L.rsrc || || ó
@ e²û►A@ {û►AM @ {û►AZ ùû►Ad 7û►An îû►Ay 7û►Aâ ADVA
PI32.d11 KERNEL32.d11 NTDLL.DLL GDI32.d11 USER32.d11 COMCTL32.d11 VERSION.d11

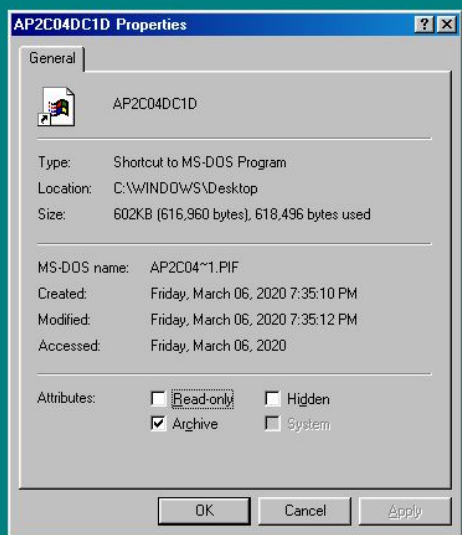
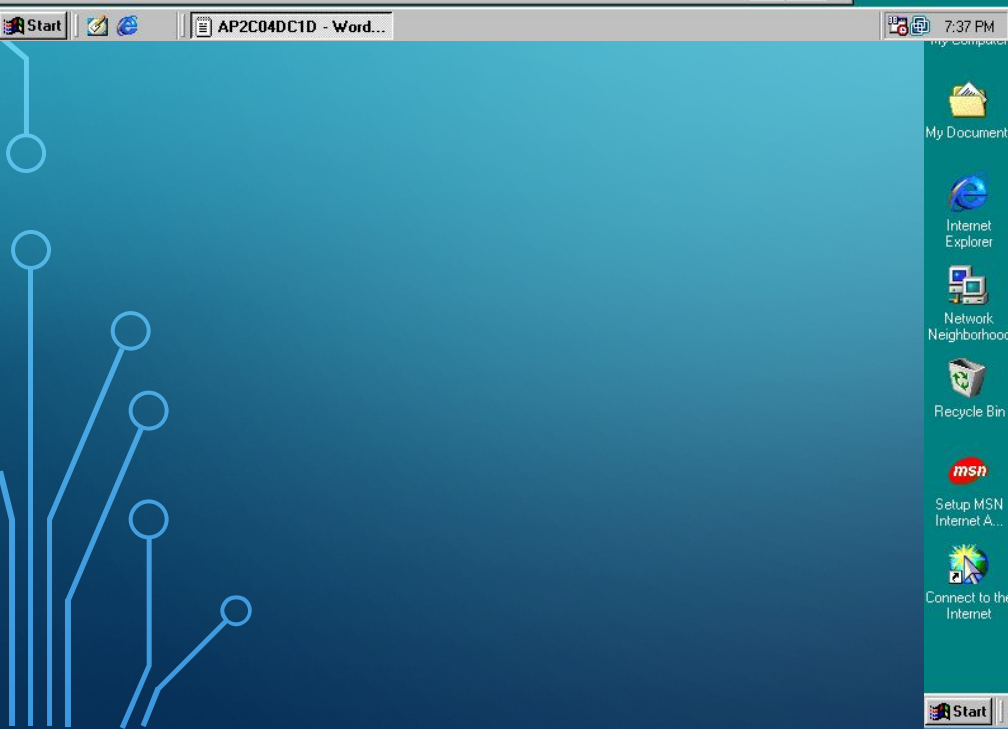
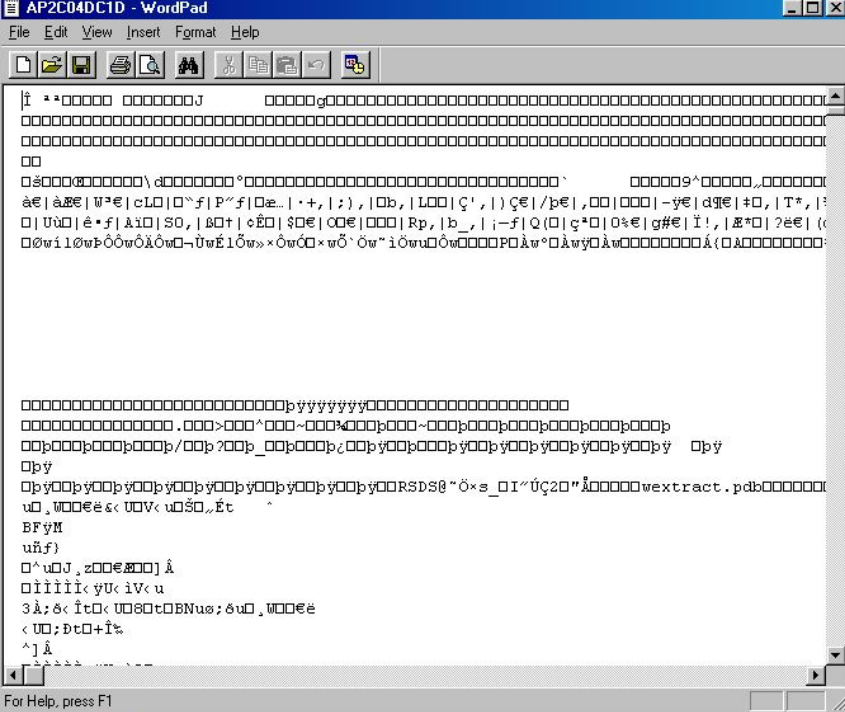
Çz| wæz| wΣ~| wv{ | wSw| w
αQ|α|Q|W|Q|cLüôâ|Pôâ|►pà|7+é|;)é|↓bé|Lxü|'é|) ||Q|/■Q|é ü|↓@ü| - Q|d||Q|gvé|T*é|↓>é
ü|U·ü|Ωôâ|ANü|SOé|■♣ã|ó♣ü|Sü|Y5ü|é fé|(¼Q|eáQ|±||Q| ||Q| |Åâ|wCQ|f*ü|²
C:\>

ANALYZING OLD MALWARE

- What tools are still available to analyze old files?
 - Nothing after Windows XP recognizes
 - Try to go back to source OS: MSDOS
 - DOSBox emulator: definitely doesn't look like just a regular file with plain text

ANALYZING OLD MALWARE

- What tools are still available to analyze old files?
 - Nothing after Windows XP recognizes
 - Try to go back to source OS: MSDOS
 - DOSBox emulator: definitely doesn't look like just a regular file with plain text
 - Windows 98, Windows XP: see if the shortcut properties give any clue to what the shortcut tries to do



AP2C04DC1D Properties

Screen

Misc


Compatibility

General

Program

Font

Memory



AP2C04DC1D

Type of file:

Shortcut to MS-DOS Program

Description:

AP2C04DC1D

Location:

C:\Documents and Settings\98Lab\Desktop

Size:

602 KB (616,960 bytes)

Size on disk:

604 KB (618,496 bytes)

Created:

Yesterday, March 04, 2020, 5:58:18 PM

Modified:

Monday, June 19, 2017, 8:51:12 AM

Accessed:

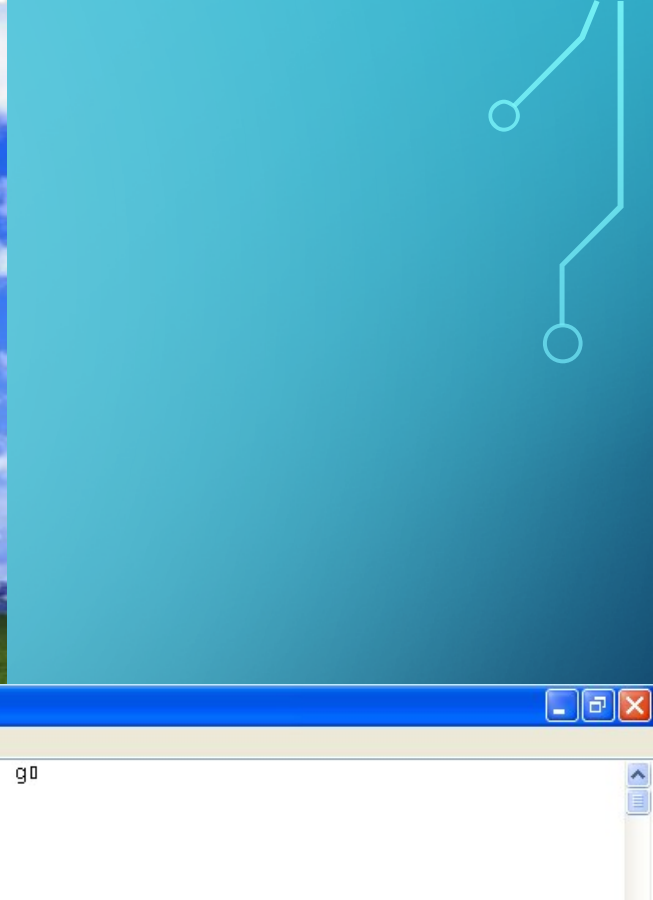
Today, March 05, 2020


Attributes:

☐ Read-only


☐ Hidden

☒ Archive





start




AP2C04DC1D - Notepad

File Edit Format View Help


```
i aa  j  go

0 yy @
$ 0a"01EUC1EUC1EUCuASC>EUC1EUC0EUCuASC.EUCuASC-EUCuA C.EUCr1ch1EUC
:),|ab,|Laa|c',|)Ccl/be|, a|aaa|-ye|dqe|+a,|t*,|%>,|)'el|a'...|xte|oaf|\ea|bu|y
ADMQCMD SHOWWINDOW REBOOT msdownld.tmp A:\DecryptFileA Control Panel
_éo9]ôtoC0û± 00 <Eð<MÜ[èHL ÉÁi1111<yU<i0i00 jð² 0%EU<E0-00 V<u0t%ht03Aék
00 oed3E9...èyyyo"A9...èyyy ± 0%00³ ouo Ñ± 0w000bpyy0psyo0 o fA0sy0@psj0j hà² oyu
0 i1111<yU<iyuoh'o oyuo0yo0 o<EgfA0]A0 i1111<yU<ifi0;jð² 0vw3y30f}00%EU<E0C0\°
Ei0,,u PjBy0"0 d;A%EU0,,A Py0"0 o<0...00,,³ Syuiyuèyu0é0x ...Atr0E0P0E0èPh0 0
0 0Py0"0 0f° 0<...èuyyc 0 0...0pyyPj0yu0úyyh0 qh00 qh00 0y00 0..Av8f0"A 0080u
>\u <\u03A0é03A\]A0 i1111<yU<ifi sv<5E0 0w3y30%}úchy jyw0E0PSyoA0 0..At6
5P° 0è0uyyf=8% 0 tofEY]Awj 0E0Pyu0<E0yu000y4A0A 0y0è0 0..Au0fiyèe<}0fytt=0=.%
^ 0 00...0pyyPyu0véc2 vyo"0 0vy0è0 0f0y<=|0 0t00000 |«è j vyx..At03A0é0E 0%..0py
="è 0è0pyyè%0pyy u0%=0E 0è0pyyè%0pyy:0...byyè%0pyy 0,,³pyy0u0pyy00Py0-0 00%Af
9v0...0pyyPyu0swy0è0 0..At0<E0;...0pyytoC0\° 0R 0è%0èpyywy0à0 0<Mü...0pyy_À[è0( ÉA
0 0v<0y0L0 0<Cé03A0<MÜ_À[èH$ ÉA0 i1111<yU<isw<=P0 0j0j0yx<030;0u0sj0ssh0
0 03A0é3j0j wsh0 wè-úyys<0y0L0 0fb0u0%=\° 0è0C0\° 0C00é3A_À[ÉÁi1111<yU<isw
0yy<u0_<A\]A0 i1111<yU<i0i 0 jð² 0v<u0%EU00..0pyy3yP%µ\byy% byyc..0pyy" y0
y0L0 0;+u0C0\° 0C00é3A00y50A 0y0L0 03A%=\° 00_À[Ái1111<yU<i0i00 jð² 0<M0s<|0
tohtà3AéU yv00..0pyyh0% 0h00 Pè'pyy..AtK3Af<F0P3Af<F0Pyv0è70yy..At4yv0èE0yy3A
0tÉ0 swwsy00 0PÉP° 0y0<0 0j0h"A 0h00 0è-0yy..At'00"A 0A0,,³ h00 0...0pyyPh
y000 0è0j yu0y000 03A0_À[]A0 i1111<yU<i<E0fè0v0,,i0 -0 0,,S0 fè00,,f Ht0-0
```

start



AP2C04DC1D - Notepad



5:35 PM

ANALYZING OLD MALWARE

- What tools are still available to analyze old files?
 - Nothing after Windows XP recognizes
 - Try to go back to source OS: MSDOS
 - DOSBox emulator: definitely doesn't look like just a regular file with plain text
 - Windows 98, Windows XP: confirmed it is an MSDOS shortcut file, but doesn't say what the shortcut goes to
 - Viewing the plain text of the file shows the same gobbledygook that we saw in the MSDos text editor

ANALYZING OLD MALWARE

- What tools are still available to analyze old files?
 - Nothing after Windows XP recognizes
 - Try to go back to source OS: MSDOS
 - DOSBox emulator
 - Windows 98, Windows XP
 - Try online sandboxes
 - Most only support Windows 7 and later
 - Any.Run gives Windows Vista option, but it is not selectable without a paid account
 - Hybrid Analysis doesn't even give an option prior to Windows 7

ANY.RUN

ANY.RUN
INTERACTIVE MALWARE ANALYSIS SERVICE

+ New task

Public tasks

FAQ

Contacts

History

Profile

Log Out

Pricing

Threat map

New Task
Let's create a new task

Choose operating system to start

- Windows 7
- Choose OS
- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10

32bit 64bit

or Choose a file

Advanced mode →

Task will be shared on the Public Submission

Run

STATISTICS FOR 24 HOURS

LockerGoga.exe
Interesting sample

2 Active tasks

3839 Total tasks

2519 No threats

170 Suspicious

1150 Malicious

Trending tags

loader rat opendll

CHANGE LOG

May 21 TODAY WE ARE READY TO RELEASE OUR API!
Now you can automate submissions and receive IOCs from your tasks in case it doesn't need user interaction. API simplifies listing of your team

RECENTLY

Http://vivekaessencemart.com/

http://203.95.192.84:9998/3.exe

Our service uses cookies. By visiting the pages of the service, you agree to our Privacy Policy

[Privacy Policy](#) [I agree](#)

The screenshot shows a virtual machine environment with a Windows 7 desktop. A large black window is open, and a smaller dialog box titled "16 bit MS-DOS Subsystem" is displayed in the foreground. The dialog box contains the following text:

```
C:\Users\admin\AppData\Local\Temp\AP2C04~1\PIF
Invalid program file name, please check your pif file. Choose 'Close' to
terminate the application.
```

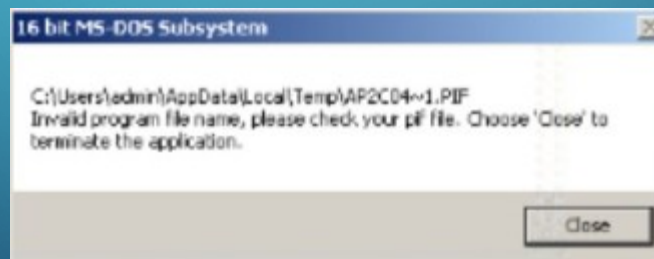
The desktop background is the standard Windows 7 blue wallpaper. The taskbar at the bottom shows the Start button and several application icons. The ANY.RUN logo is visible in the bottom right corner of the desktop.

The screenshot shows the ANY.RUN web interface. At the top, the file name "AP2C04DC1D.pif" is displayed with an "INFO" button. Below it, the MD5 hash "FBA741EDA2751DA52F5ACC35692EBDB6" and the start time "12 SEPTEMBER 2019, 17:52" are shown. A "Total: 60 s" indicator is also present. A "No threats detected" message is visible in the top right corner.

The interface includes several tabs for analysis: "ENVIRONMENT", "Sample", "IOC", "Re-run", "Export", "Reports", and "ATT&CK™ matrix". The "ENVIRONMENT" tab is currently selected, showing a "CPU" section with a progress bar.

The "PROCESS" section is visible, showing a list of processes. The first process listed is "ntvdm.exe -11" with a PID of 3052. The interface also includes a "Filter by name or PID" input field and a "Show only important" checkbox.

At the bottom of the interface, there is a banner that reads "Get more awesome features with premium access!" and a "REVIEW" button.



HYBRID ANALYSIS

Sandbox ▾ Quick Scans ▾ File Collections ▾ Resources ▾ Request Info ▾ More ▾

Analysis Environments

Name AP2C04DC1D.pif
Size 602.5KiB
Type **data** ⓘ
MIME application/octet-stream
SHA256 b172582956deca...5805b000ad89b ⓘ

Available:

VMs

- ☒ Windows 7 32 bit 2/71
- ☐ Windows 7 32 bit (HWP Support) ⓘ 2/70
- ☐ Windows 7 64 bit 0/70
- ☐ Linux (Ubuntu 16.04, 64 bit) 0/18
- ☐ Android Static Analysis
- ☐ Quick Scan ⓘ 3/3

There are 2 files in the processing queue.
Currently, the average processing time per sample is 6 minutes and 30 seconds seconds.

« Back

Runtime Options ⓘ

Generate Public Report ⓘ

<http://www.example.com/suspicious.zip>



Analyze

Falcon Sandbox Reports

ERROR

⊘ AP2C04DC1D.pif

Analyzed on: 09/12/2019 21:33:14

Environment: Windows 7 32 bit



If you believe this is incorrect behavior, please
contact support@hybrid-analysis.com providing the
SHA256 and sample.

[Analysis Overview](#)[Anti-Virus Scanner Results](#)[Falcon Sandbox Reports \(1\)](#)[Community \(0\)](#)[Back to top](#)

Analysis Overview

[Request Removal](#)

Submission name: b172582956deca61b8da9a9cc52e9cd954125c3aa8056974cbb5805b000ad89b ⓘ
 Size: 603KiB
 Type: [data](#) ⓘ
 Mime: application/octet-stream
 SHA256: b172582956deca61b8da9a9cc52e9cd954125c3aa8056974cbb5805b000ad89b ⓘ
 Last Sandbox Report: -

malicious

AV Detection: 6%
 Labeled as: Trojan.Generic

[Link](#)
[Twitter](#)
[E-Mail](#)

Analysis Overview

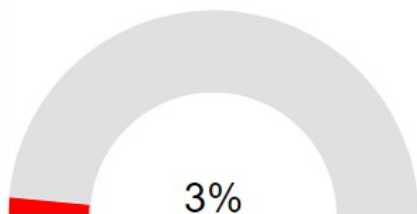
Anti-Virus Scanner Results
 Falcon Sandbox Reports (1)
 Community (0)

[Back to top](#)

Anti-Virus Results

[Refresh](#)

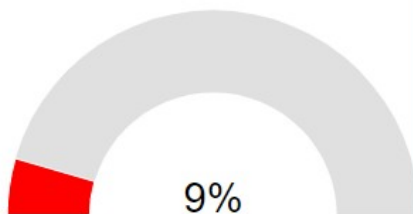
MetaDefender



Multi Scan Analysis

Last Update: 09/12/2019 23:40:51

VirusTotal



Multi Scan Analysis

Last Update: 09/12/2019 23:40:51

ANALYZING OLD MALWARE

- What tools are still available to analyze old files?
 - Nothing after Windows XP recognizes
 - Try to go back to source OS: MSDOS
 - DOSBox emulator
 - Windows 98, Windows XP
 - Try online sandboxes
 - Virus total gives some confirmation that it is a bad file



URL, IP address, domain, or file hash



Sign in



5 engines detected this file



b172582956deca61b8da9a9cc52e9cd954125c3aa8056974cbb5805b000ad89b
AP2C04DC1D.pif

602.5 KB
Size

2019-09-12 21:28:10 UTC
1 minute ago



DETECTION

DETAILS

COMMUNITY

Avast

Win32:Rootkit-gen [Rtk]

AVG

Win32:Rootkit-gen [Rtk]

ClamAV

Win.Malware.Yakes-6895522-0

eScan

Dropped:Trojan.GenericKD.5055052

NANO-Antivirus

Trojan.Win32.GenericKD.eoqnab

Ad-Aware

Undetected

AegisLab

Undetected

AhnLab-V3

Undetected

ALYac

Undetected

Antiy-AVL

Undetected

Arcabit

Undetected

Avast-Mobile

Undetected

Avira (no cloud)

Undetected

Baidu

Undetected

WHAT DID I LEARN?

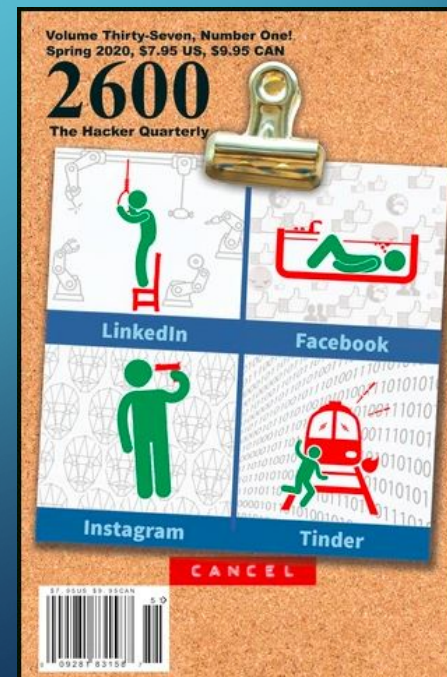
- It is very difficult to do casual malware analysis on old file types
 - Don't have easy access to supported systems to examine the file
 - Automated malware analysis systems don't support the old systems either
- If you do need to analyze an old unsupported file, try VirusTotal
- Then call in a malware analyst

SO WHAT CAN YOU DO?

- Don't run suspicious files from email attachments
- Get necessary old files from trusted sources
 - From the manufacturer
 - Make sure to confirm the file hash is correct
 - Not from file sharing sites

MORE INFO

- An article about my analysis is also in the Spring 2020 issue of 2600 magazine.



The background is a blue gradient. In the corners, there are white line art designs resembling circuit boards or neural networks, with lines and small circles.

Any Questions?